Amendments to the Claims

Please replace the Claims as shown below:

1. (Currently Amended) A processor ~~with secure cryptographic capabilities, said processor~~ comprising:

a digital secret including a secret key used in a key-based cryptographic process, wherein the digital secret is stored [[only]] within the processor, [[and]] wherein the processor is configured to use the digital secret ~~is operable to be used exclusively by the processor~~ for both encryption and decryption, wherein the digital secret is calculated using an HMAC algorithm implemented on testing data, and wherein the testing data is associated with fabrication of the processor;

a cryptography engine ~~for performing~~ configured to perform the key-based cryptographic process internally within the processor~~, wherein the cryptography engine is configured to access~~ using the digital secret; and

internal memory ~~coupled to the cryptography engine and~~ configured to ~~support the key-based cryptographic process, wherein the internal memory is further configured to~~ store data associated with the key-based cryptographic process, wherein the data includes at least one result of a calculation performed by the key-based cryptographic process~~, and wherein the data is accessible only within the processor~~.

2. (Previously Presented) The processor of Claim 1 further comprising an internal bus configured to facilitate secure communication between the cryptography engine, the digital secret, and the internal memory within said processor.

3. (Previously Presented) The processor of Claim 1, wherein the digital secret is securely confined within the processor.

4. (Previously Presented) The processor of Claim 1, wherein the internal memory includes microcode for implementing the key-based cryptographic process on the data within the processor, and wherein the internal memory is configured to perform state tracking associated with the key-based cryptographic process.

5. (Previously Presented) The processor of Claim 1, wherein the data includes intermediate data generated by the key-based cryptographic process.

6. (Previously Presented) The processor of Claim 1 further comprising:

a cryptography unit including a functional unit within the processor for securely executing the key-based cryptographic process internally within the processor, wherein the cryptography unit includes:

the digital secret;

the cryptography engine; and

the internal memory.

7. (Previously Presented) The processor of Claim 1, wherein the key-based cryptographic process includes:

a key-based encryption process; and

a key-based decryption process.

8. (Currently Amended) The processor of Claim 1, wherein the processor includes:

a secure hardware environment configured to provide core processing functionality; and

a secure software environment coupled to the secure hardware environment, wherein the secure software environment is configured to generate executable instructions that are sent to the secure hardware environment for processing, wherein the secure hardware environment in combination with the secure software environment is configured to provide processor capability, and wherein the secure hardware environment is accessible [[only]] through the secure software environment.

9. (Previously Presented) The processor of Claim 1, wherein the digital secret is unique to the processor and is permanently and physically manifested within the processor.

10. (Currently Amended) A processor ~~with cryptographic capabilities, said processor~~ comprising:

a secure cryptography unit, wherein the cryptography unit is configured to internally provide secure cryptographic capabilities as a functional unit within the processor, the cryptography unit including:

a cryptography engine configured to perform a key-based cryptographic process;

a digital secret ~~exclusively~~ accessible to the cryptography engine, wherein the digital secret includes a secret key used in the key-based cryptographic process, [[and]] wherein the processor is configured to use the secret key ~~is configured to be used exclusively by the processor~~ for both encryption and decryption, wherein the digital secret is calculated using an HMAC algorithm implemented on testing data, and wherein the testing data is associated with fabrication of the processor; and

internal memory ~~coupled to the cryptography engine and~~ configured to ~~support the key-based cryptographic process, wherein the internal memory is further configured to~~ store data associated with the key-based cryptographic process, wherein the data includes at least one result of a calculation performed by the key-based cryptographic process~~, and wherein the data is accessible only within the processor~~.

11. (Previously Presented) The processor of Claim 10, wherein the key-based cryptographic process includes:

a key-based encryption process; and

a key-based decryption process.

12. (Previously Presented) The processor of Claim 10, wherein the processor is a very long instruction word (VLIW) processor.

13. (Currently Amended) The processor of Claim 10, wherein the processor includes:

a secure hardware environment providing core processing functionality; and

a secure software environment coupled to the secure hardware environment, wherein the secure software environment is configured to generate executable instructions that are sent to the secure hardware environment for processing, wherein the secure hardware environment in combination with the secure software environment is configured to provide processor capability, and wherein the secure hardware environment is accessible [[only]] through the secure software environment.

14. (Previously Presented) The processor of Claim 10, wherein the digital secret is unique to the processor and is permanently and physically manifested within the processor.

15. (Previously Presented) The processor of Claim 10, wherein the digital secret includes:

a plurality of fusible links configured to manifest the digital secret by permanently setting a binary state in each of the plurality of fusible links.

16. (Canceled)

17. (Currently Amended) The processor of Claim [[16]] 10, wherein the testing data includes:

wafer test data; and

die test data.

18. (Previously Presented) The processor of Claim 10, wherein the secure cryptography unit is a fully integrated circuit within the processor.

19. (Previously Presented) The processor Claim 10, wherein the digital secret and the internal memory are fully integrated with the cryptography engine to facilitate communication without use of a bus.

20. (Previously Presented) The processor of Claim 10, wherein the key-based cryptography process includes a Triple Data Encryption Algorithm (TDEA or Triple DES) cryptography process.

21. (Currently Amended) A processor ~~with secure cryptographic capabilities~~, ~~the processor~~ comprising:

a secure hardware environment configured to provide core processing functionality, wherein the secure hardware environment includes:

a secure cryptography unit configured to provide secure cryptographic capabilities as a functional unit within the secure hardware environment, wherein the secure cryptography unit is configured to facilitate performance of a key-based cryptographic process performed ~~exclusively~~ by the processor, wherein the key-based cryptographic process includes encryption using a digital secret and decryption using the digital secret, wherein the digital secret is calculated using an HMAC algorithm implemented on testing data, wherein the testing data is associated with fabrication of the processor, wherein the key-based cryptographic process further includes generating data, wherein the data includes at least one result of a calculation performed by the key-based cryptographic process~~, and wherein the data is accessible only within the processor~~.

22. (Previously Presented) The processor of Claim 21 further comprising:

a secure software environment configured to access the secure hardware environment, wherein the secure software environment is configured to generate executable instructions that are sent to the secure hardware environment for processing, wherein the secure hardware environment in combination with the secure software environment is configured to provide processor capability.

23. (Currently Amended) The processor of Claim 21, wherein the secure cryptography unit includes:

a cryptography engine configured to perform the key-based cryptographic process;

the digital secret accessible ~~exclusively~~ to the cryptography engine, wherein the digital secret includes a secret key used in the key-based cryptographic process; and

internal memory coupled to the cryptography engine, wherein the internal memory is configured to support the key-based cryptographic process and further configured to perform state tracking associated with the key-based cryptographic process.

24. (Previously Presented) The processor of Claim 23, wherein the internal memory is configured to securely store the data, and wherein the data includes intermediate data generated by the key-based cryptographic process.

25. (Previously Presented) The processor of Claim 21, wherein the secure cryptography unit is a fully integrated circuit within the processor.

26. (Previously Presented) The processor of Claim 23, wherein the secure cryptography unit is a fully integrated circuit within the processor, and wherein the secure cryptography unit is configured to facilitate communication between the cryptography engine, the digital secret and the internal memory without use of a bus.